7. ABSTRACT

The subject of the disclosed technology is, when a crypto-processing is performed utilizing an information processing device buried in an IC card, etc., to decrease the relationship between the waveform of the consumption current and the contents of the crypto-processing as a countermeasure against a tamper which observes the waveform of a consumption current.

A solution means is shown in the following. When a decryption processing of an RSA cryptogram is performed according to CRT, in step 608, for every unit bit block of XP a modular exponentiation calculation is performed, and the partial result of CP up to the calculated bit block is stored in a memory. In step 609, for every unit bit block of XQ a modular exponentiation calculation is performed and the partial result of CQ up to the calculated bit block is stored in a memory. In step 606, a random number is generated, and in step 607, it is decided that step 608 is to be executed or step 609 is to be executed corresponding to the value of the random number.